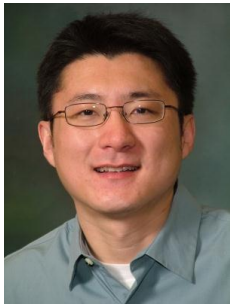
SPARCHS: Hardware Support for Software Security







Sal Stolfo

Department of Computer Science

Columbia University

SPARCHS* Guiding Principle

Current Security	*SPARCHS Security*
• **Reactive** – "Show me a real-life incident"	• **Proactive** – Protect against known & unknown attacks
• **Top-down** – Most attention to the most exposed layers	• **Bottom-up** – Hardware support for software security
• **Security as an add-on** – "Asserts" are removed – AV/IDS shutdowns	• **Security from get go** – Assume flaws exist – Defend the defenses

*Symbiotic, Polymorphic, Autotomic, Resilient, Clean-slate, Host Security

SPARCHS: Clean-slate security

Advances

- **Hardware support for dynamic diversity, protected execution, recovery & adaptive learning**
- **Challenge: Is this enough?**

Benefits

- **Cover common sources of insecurity**
- **Lack of security, buggy security or static security**

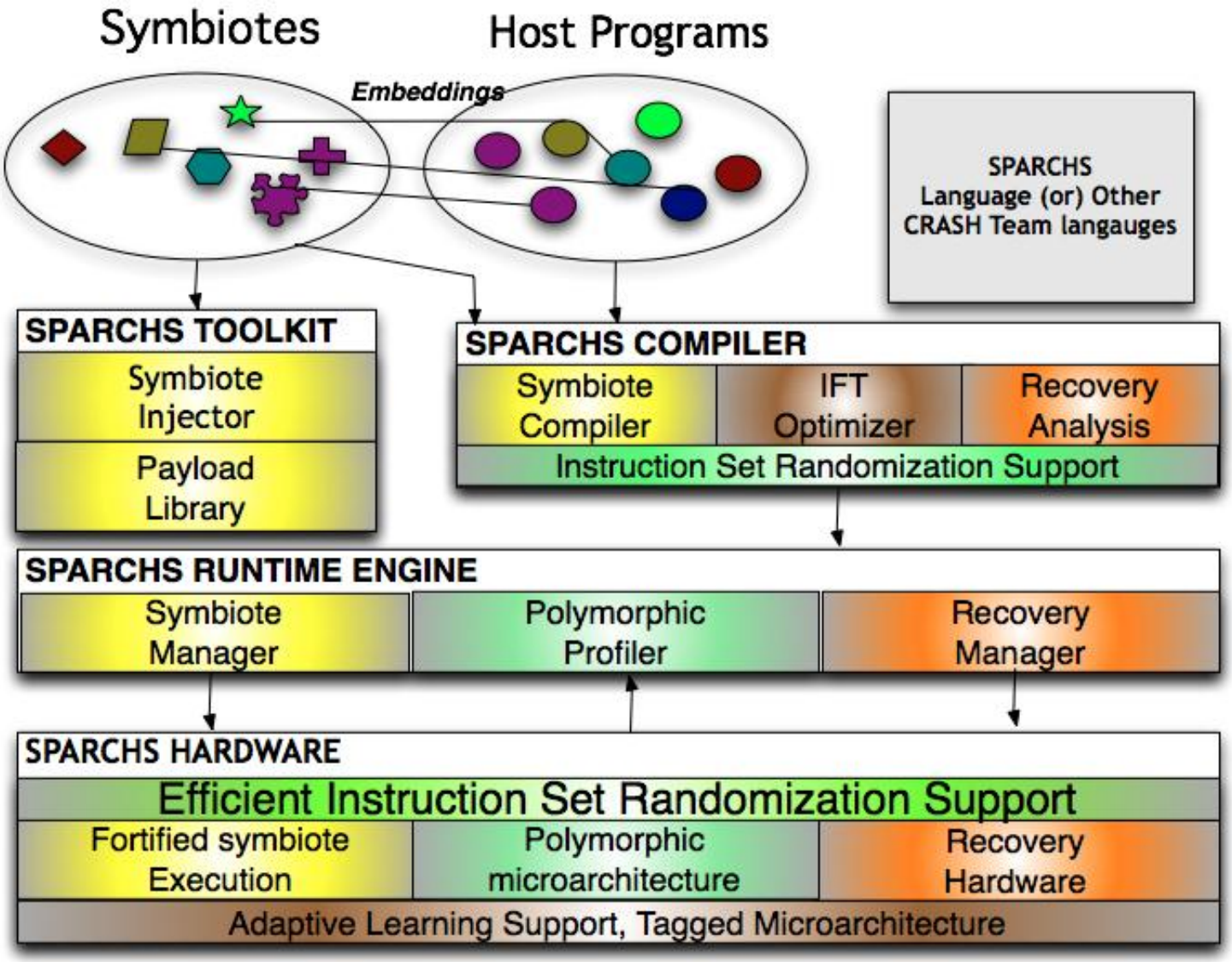
Context

- **Multi/Many-core architectures; serial and parallel codes**
- **Energy-efficiency and reliability constraints**

Bio Security & Analogues

- **Innate Immunity**
  - Body "knows" local and foreign organisms
  - Better information flow tracking
  - Track *implicit* flows with improved static analysis; and better performance
- **Adaptive Immunity**
  - Body learns from past attacks
  - Support for Adaptive Learning
  - Improve processor's ability to monitor software execution
- **Symbiotic Immunity**
  - A new type of immunity inspired by microbiomes
  - Every program must have a security symbiote
  - Symbiote encapsulates security function
- **Defensive Polymorphism**
  - Shape-shifting hardware and software for diversity including ISR
  - Inspired by shape-shifting viruses in nature (e.g., HIV, Cold)
  - Protects against deterministic and non-deterministic bugs
- **Defensive Autotomy (not mispelled)**
  - Lose non-critical functions under attack
  - Hardware and software for continued operation
  - Expensive but useful e.g., lizards dropping tails

Integrated SPARCHS System



Status

- Four year, multi PI project, 2 quarters completed
  - Adaptive Immunity
    - Released a low-overhead tool that will allow x86 performance counters to be read. Useful for adaptive learning. [ISCA 11]
  - Dynamic Polymorphism
    - Released a software prototype of Instruction Set Randomization. Precursor to HW prototype.
  - Innate Immunity
    - Very fast IFT nearing release. Almost zero overhead
  - Symbiotic Immunity
    - Created embedded and system level attacks to demonstrate utility of software symbiotes
- We are looking for PhD students, Post Docs, Engineers and Collaborators. Much more exciting work to be done.
  - Contact: simha@cs.columbia.edu, sal@cs.columbia.edu
  - Learn more: http://castl.cs.columbia.edu/sparchs